The Quarterly Magazine for Digital Forensics Practitioners

Issue 28 • August 2016

DIGITAL FORENSICS / MAGAZINE

WIN! an iPod Nano

Log Extraction and Analysis of CHROMECAST 2.0

Latest News, 360
Book Reviews, IRQ
& much more inside!

PLUS!

Mathematica
Careers in Cyber Security
Embedded Computing
Cloud Honeypots

9 772042 061004 28
Issue 28 / £14.99 TR Media

/ FEATURE

CLOUD HONEYPOTS

"How feasible is a distributed Honeypot Deployment in The Cloud?" asks Simon Clary and Adrian Winckles.

/ INTERMEDIATE

The exponential growth of the Internet over recent years has had a revolutionary effect on many areas of society from commerce to the political landscape, but this growth has also been combined with a growth of online crime or cybercrime, which includes an ever widening array of malicious activities such as fraud, extortion and industrial espionage.

One of the main techniques of cybercriminals is the spread of malicious software, which has been given the umbrella term malware. Computers are usually infected through malicious code, unpatched vulnerabilities in the operating system and backdoors left by malware. Both the size and the frequency of the malicious attacks are increasing and are now being used for geo-political as well as criminal purposes (Mansfield-Devine. 2011).

As the threat of cybercrime has increased many methods of studying the nature of the threat as a means to find countermeasures have been evaluated. One tool commonly employed by researchers and by private companies is honeypots.

/ HONEYPOTS

"A honeypot is a closely monitored computing resource that we want to be probed, attacked, or compromised. More precisely, a honeypot is an information system resource whose value lies in unauthorised or illicit use of that resource."

In essence a honeypot is a passive computer system with a number of different sensors and monitoring tools in place; because it is non-active technically there should be no communication with the system therefore all activity with the honeypot from outside has the potential to be considered malicious (Spitzner, 2002). A collection of honeypots is known as a 'honeynet'.

Honeypots have been classified into two categories depending on their role:

1. Production Honeypots – whose role is to help protect a systems of an organisation by being a decoy or by providing information about attacks
2. Research Honeypots – used by security researchers to predict new trends in attacks, possible targets and new vulnerabilities. (Mokube and Adams, 2007)

Also, typically Honeypots have been classified into three categories depending upon their functionality [Tablee 1]:

1. Low interaction honeypots – Basic emulated systems
2. Medium interaction – Emulated systems with limited interaction
3. High interaction honeypots – Real systems with full interaction

/ THE CLOUD

One of the major advances in computing in recent years has been the development of cloud computing. Cloud Service Providers typically offer both refined software services such as databases, as well as raw computing resources such as storage or processing power, provided over the Internet. Such services create big advantages for individuals and organisations in terms of cost, scalability and computing capacity.

/ KIPPO

Kippo is a medium interaction honeypot, which means that it imitates some functions of a real Linux system. Its main focus is to emulate the SSH service. It contains the ability to create a fake file system and as well as logging all the details of the SSH attack such as the IP address of the attacker, logs any commands entered and creates a recording of the entire shell interaction and saves any files or malware downloaded as a binary. (Desaster, 2015)

/ DIONAEA

Dionaea is a low interaction honeypot whose main purpose is to emulate services of a vulnerable network, which mimics a vulnerable Windows 2000 system and emulates a number of different protocols such as SMD, HTTP, FTP, TFTP, MSSQL, MYSQL and SIP. Although it collects a number of different sets of data its primary function is that of collecting malware samples. (Dionaea, 2013)

/ GLASTOPF

Glastopf is a low-interaction honeypot which emulates a basic vulnerable web server. The honeypot collects information about web application based attacks like remote file inclusion, SQL injection and local file inclusion attacks. It is programmed to respond appropriately to attackers and download samples of any malware.

Level of Interaction	Work to Install and configure	Work to Deploy and Maintain	Information Gathering	Level of Risk
Low	Easy	Easy	Limited	Low
Medium	Involved	Involved	Variable	Medium
High	Difficult	Difficult	Extensive	High

Table 1. Honeypot Levels of Interaction (Spitzner, 2002)

“BOTH THE SIZE AND THE FREQUENCY OF THE MALICIOUS ATTACKS ARE INCREASING AND ARE NOW BEING USED FOR GEO-POLITICAL AS WELL AS CRIMINAL PURPOSES.”

Typically in the past the system resources available limited the deployment of research honeypots, but with the advent of cloud computing the deployment of honeypots at a much wider scale is potentially much easier, scalable and economical than in the past.

/ THE AIMS OF THIS STUDY

The purpose of this study is to find out how feasible a distributed deployment of honeypots in the cloud is and to analyse what useful data such a deployment can be obtained to aid in the fight against cybercrime and malware distribution.

/ HOW THE STUDY WAS CONDUCTED

After a period of evaluation and testing the three honeypots chosen were:

- Kippo (Desaster, 2015), which monitors SSH brute force attacks on a Linux system
- Dionaea (Dionaea, 2013) which emulates many vulnerabilities of a Windows server
- Glastopf (Glastopf, 2015), which emulates a vulnerable web server.

The types of data intended to be recorded, were:

- Who is typically attacking the systems
- How they are attacking, how they break in
- What they do once they break into a system
- Analysis of the malware and malicious activity attempted within the system

The study was separated into two stages. The first stage was to set up four Kippo honeypots for 30 days. The second stage was to set up four Dionaea honeypots and two Glastopf honeypots for a period of 16 days. All the honeypots were deployed on Amazon EC2 cloud instances.

Honeypot	Type	OS	Language	GUI	License
Honeyd	Generic	LINUX	C	N	GNU
Nepenthes	Malware	LINUX	C	N	GNU
Dionaea	Malware	LINUX	PYTHON	N	GNU
Honeytrap	Generic	LINUX	C	N	GNU
LaBrea	Generic	LINUX	C	N	GNU
Tiny HP	Generic	LINUX	PERL	N	GNU
HoneyBot	Malware	WINDOWS	-	Y	CLOSED
Google Hack HP	WEB	-	PHP	Y	GNU
Multipot	Malware	WINDOWS	VB 6	Y	GNU
Glastopf	WEB	-	PYTHON	Y	GNU
Kojoney	SSH	LINUX	PYTHON	N	GNU
Kippo	SSH	LINUX	PYTHON	N	BSD
Amum	Malware	LINUX	PYTHON	N	GNU
Omnirova	Malware	WINDOWS	Borland Delphi	Y	GNU
BillyGoat	Malware	-	?	?	CLOSED
Artemisa	VOIP	-	PYTHON	N	GNU
Ghost	USB	WINDOWS	C	Y	GNU

Table 2. Current State of Honeypot Software (Koniaris, 2013)

The study manages to demonstrate that although there are limitations and difficulties, it is feasible to deploy a range of honeypots in the cloud, which may obtain a wide range of information and data to help provide intelligence in the battle against cybercrime.

/ METHODOLOGY

Honeypot selection

Creating a high interaction honeypot in the cloud is difficult as you are limited with the hardware and software available and there are potential legal issues if the honeypot becomes compromised and used as a platform to mount attacks on other users. Therefore low and medium interaction research honeypots were more ideal for the purpose of this study.

There are a large number of honeypots available, the majority are open source, which means that many of them are not maintained or receive updates, and many lack documentation and guides for new users. [Table 1]

Recommendations

The most commonly used honeypot in the academic research reviewed was the malware honeypot called Nepenthes. Unfortunately, it is now obsolete. Its successor is considered to be the Dionaea honeypot.

A study conducted by Brown, et al, (2012) did a comparison of the main honeypots available and came to the conclusion that:

“Dionaea and Kippo performed very well and produced copious amounts of useful data. The other honeypots, Amun, Artillery, and Glastopf, were not as effective, given that they received little traffic beyond port scans.”

The European Network and Information Security Agency (ENISA) conducted an in depth survey of 30 different honeypots. The study concluded; “The most important are a group of the most mature and ready to use honeypots: Dionaea , Glastopf , kippo and Honeyd .” (Grudziecki et al, 2012). Due to its design and intentions Honeyd is more suited for an off cloud setting.

Selection

After taking into consideration all the variables and recommendations, plus after some considerable testing it was decided that Kippo, Dionaea and Glastopf would be chosen for this study for the range and detail of data they can collect and for their ease and appropriateness for deployment at scale in a cloud environment. With this choice there is one Linux emulation honeypot, one Windows emulation and one web-application honeypot.

Choice of Cloud Provider

Upon analysis the main market leading companies and the older more mature companies tend to have the best resources and support available and provide a wider range of features. Amazon EC2 is currently the clear market leader (Gartner, 2014).

The comparison made by Brown et al (2012) found they had problems setting up honeypots with IBM Smartcloud and found that for Linux operating systems Amazon EC2 was a lot cheaper than Windows Azure and found configuration easier on EC2. Amazon also provides an easy to use control panel to create, clone, edit and remove instances with ease

Overall it was considered that Amazon EC2 was the best choice of Cloud provider to use for this study.

Testing

All the three types of honeypot were tested with two instances for a minimum of two weeks each to ensure correct configuration and reliable data capture.

Development and Deployment

To ensure that the honeypots were not on the same physical computer architecture for security and reliability reasons and for a general comparison, a diverse range of geographical locations were chosen. The regions selected for were:

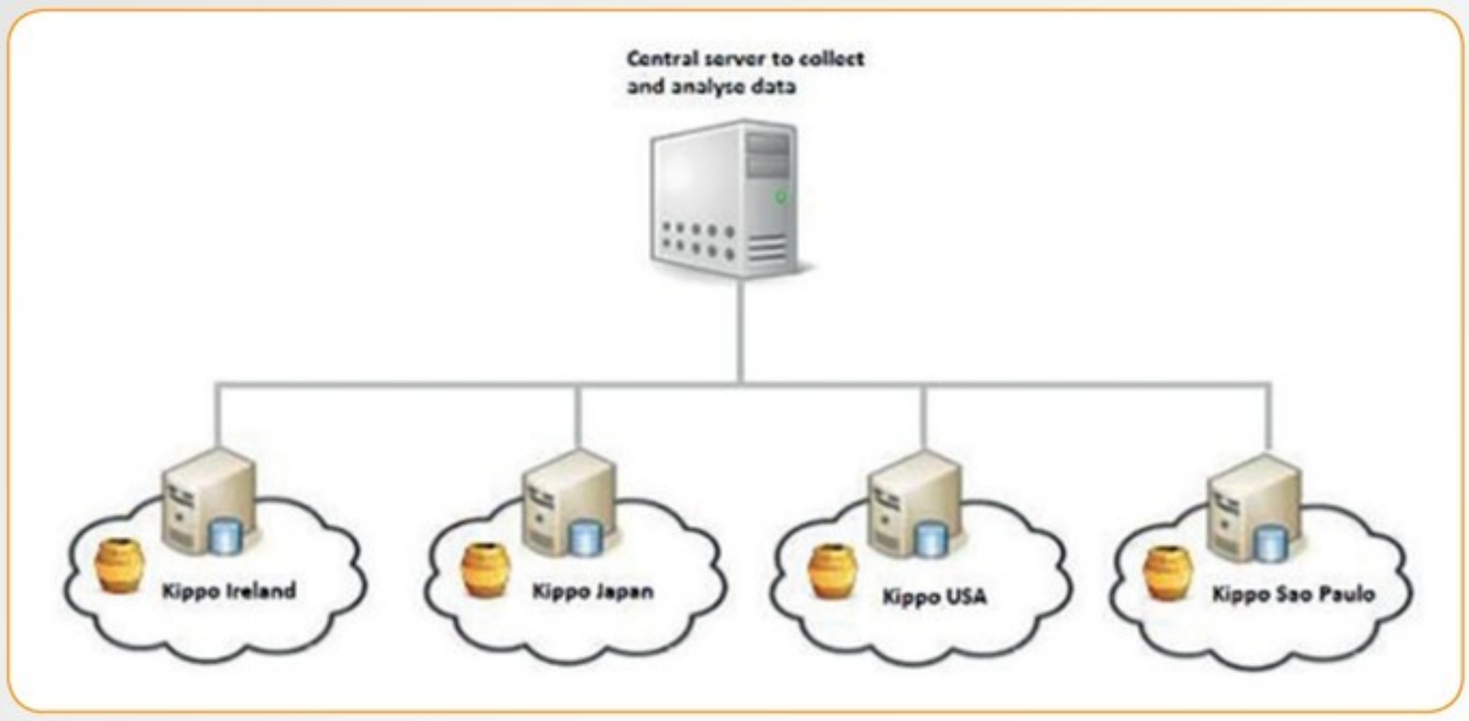


Figure 1. Kippo Deployment Structure

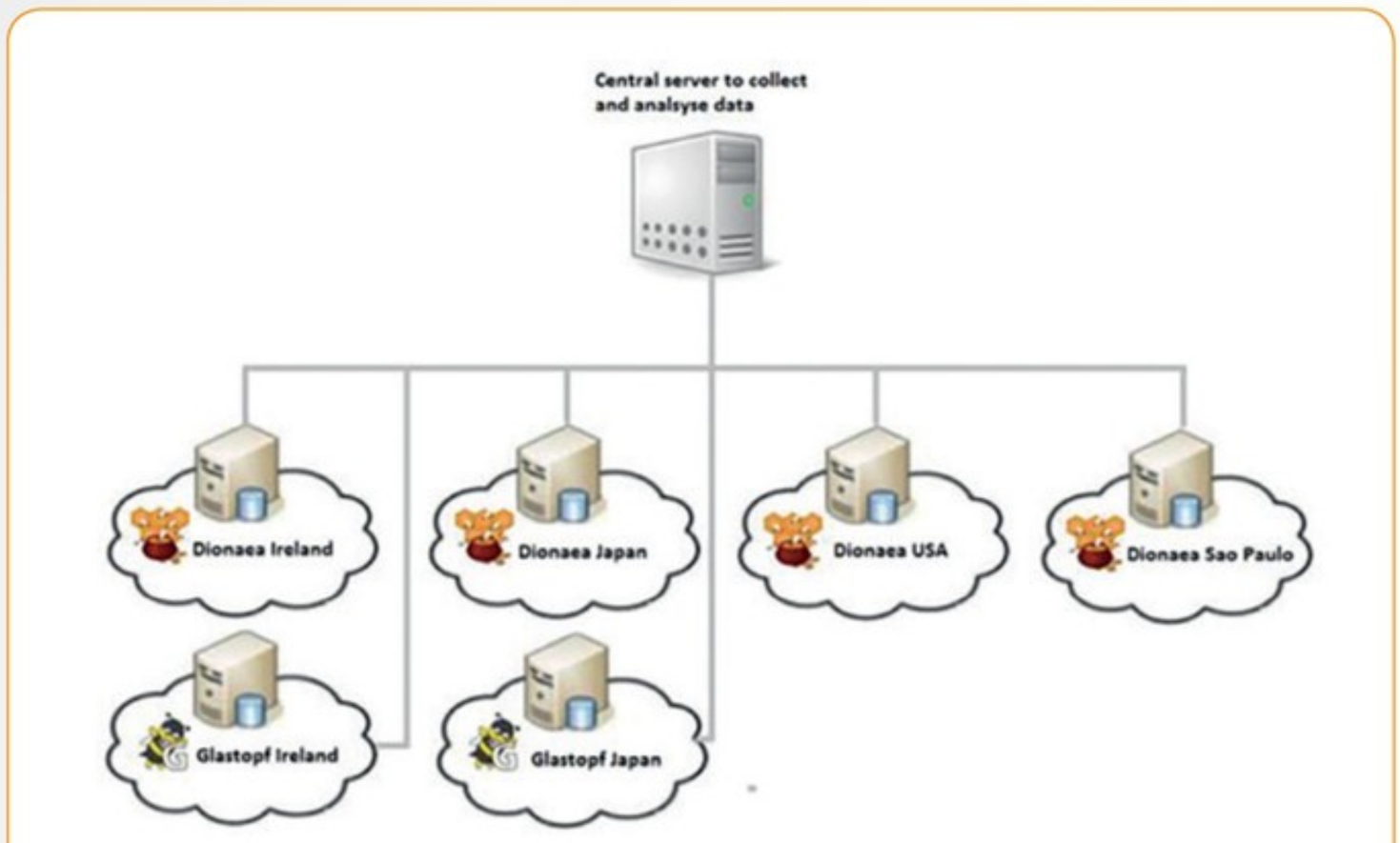


Figure 2. Dionaea & Glastopf Deployment

- EU (Ireland)
- Asia Pacific (Tokyo)
- US West (N. California)
- South America (Sao Paulo)

It was decided to deploy the honeypots in two phases:

1. Deployment of four Kippo honeypots, one in each region. [Figure 1]
2. Deployment of four Dionaea honeypots with one in each region and two Glastopf honeypots, one in Ireland and one in Tokyo. [Figure 2]

/ AMAZON CLOUD CONFIG.

All of the honeypots were created using Amazon EC2 free tier Virtual Servers. The Ubuntu Linux operating system were chosen (Ubuntu Server 14.04 LTS (HVM), SSDD Volume Type) with 8 GiB of storage. Each honeypot was given its own static IP address.

The security settings were configured as follows:

- Kippo servers – Port 22 (Fake kippo SSH) left open Port 49160 (real SSH access) public key access only to the real system
- Dionaea servers – Ports 21 (FTP), 22 (SSH) , 80 (HTTP), 135 (DCE), 443 (HTTPS) , 445 (SMB), 3306 (MYSQL), 1433 (MS SQL), left open Port 65534 (real SSH access) public key access only to the real system
- Glastopf servers – Ports 80 (HTTP) , 443 (HTTPS) left open Port 22 (SSH) public key access only to the real system

/ HONEYPOT CONFIGURATION

Kippo

Due to Kippo being a medium interaction honeypot it has more options and variables in its configuration. It was considered more important to create the perspective of the

honeypot being as realistic as possible so as to fool any human attackers, therefore small modifications were necessary to enable adequate subterfuge which included altering default configuration settings such as the password, server name, creating fake file structure and fake files

Dionaea

Even though there are less configuration variables which can be modified the creation of the Dionaea honeypots on a cloud setting proved more difficult and the first round of Dionaea deployment had to be scrapped after a week when it was discovered that they weren't recording data properly. This was mostly due to the lack of guides and documentation available to help the setting up on the latest Ubuntu platforms available on the cloud setting. Otherwise it was set up with default settings

Glastopf

Configuring the Glastopf honeypots proved that what was required was to download some extra dependencies in addition to the standard installation to ensure it can run on the latest version of Ubuntu servers. In order to increase the likelihood of the web honeypots getting noticed the sites were "advertised" by submitting their url IP to Google services.

/ CENTRAL SERVER CONFIGURATION

All the honeypots were configured with Linux bash scripts to save a copy of their database daily on their cloud server, then the central database was configured to download them daily by scp protocol.

All databases were analysed using a number of tools, scripts and automated front-end management programs including:

- Phpmyadmin
- PhpliteAdmin
- Kibana and Elasticsearch – An analytic platform (Elastic. 2015)
- Kippo-graph – Used to visualise many Kippo statistics and playback video shell interactions from localhost address in web browser (Brute Force, 2015)
- DionaeaFR – A tool for Dionaea to visualise some of the data from the database (Ruben Espadas, 2013)

Total login attempts:	1,296,447
Total successful login attempts:	100
Distinct source IP addresses:	732
Malware samples downloaded:	15

Table 3. Kippo Total/Comparison between individual honeypots

Figure 3. Total Kippo Login Attempts by Honeypot

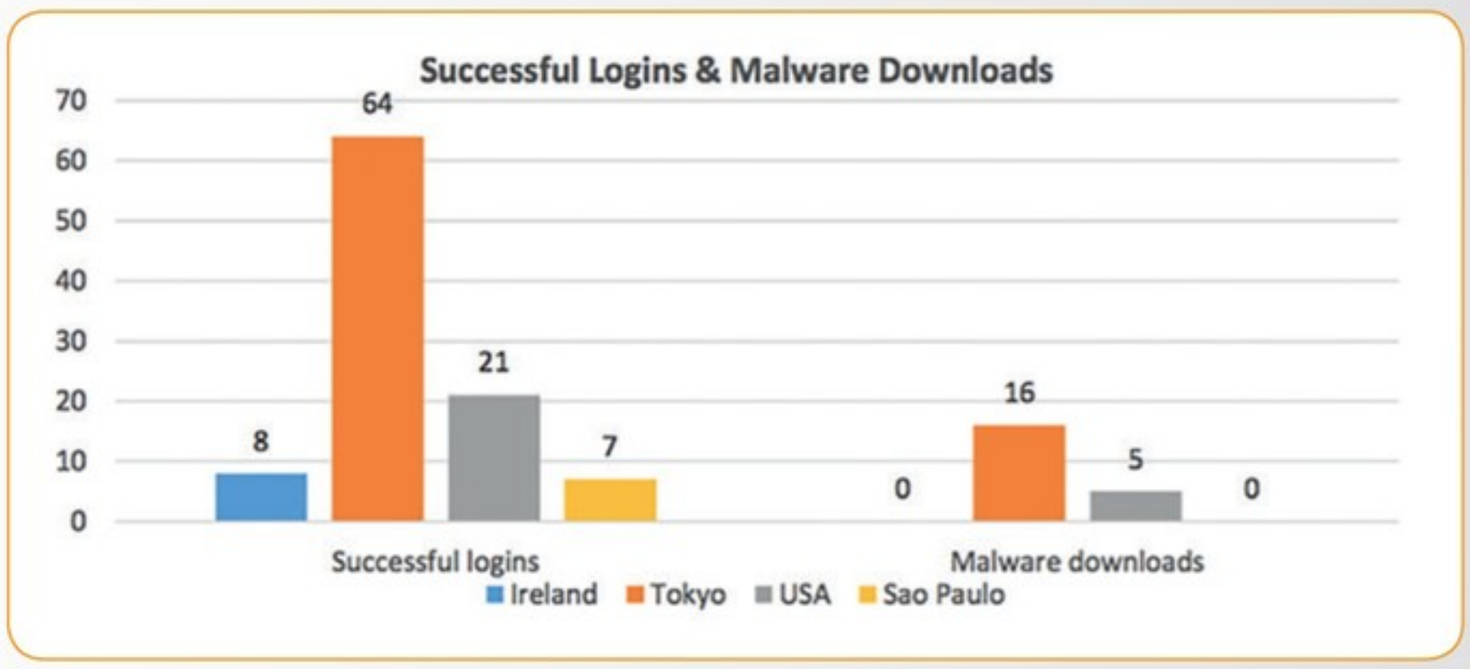


Figure 4. Kippo Successful Logins & Malware Downloads

IP addresses were examined using:
http://whois.domaintools.com/
http://www.mcafee.com/threat-intelligence/ip/

Malware samples were sent to:
https://www.virustotal.com/
https://malwr.com

/ RESULTS PHASE 1 – KIPPO

All four Kippo honeypots ran uninterrupted except for occasional brief periods of maintenance. They ran between 1-30 March 2015, for 30 days in total and received close to 1.3 million probes. [Table 3 & Figure 3]

While SaoPaulo had the most probes it was in the Tokyo instance where those attacking had most success in getting access and downloading malware. [Figure 4]

"ONE NOTABLE FIND WAS THAT ONE OF THE ATTACKERS LEFT THEIR SERVER INFORMATION WHEN TRYING TO DOWNLOAD MALWARE, WHICH REVEALED A BOTNET CREATION AND CONTROL PANEL."

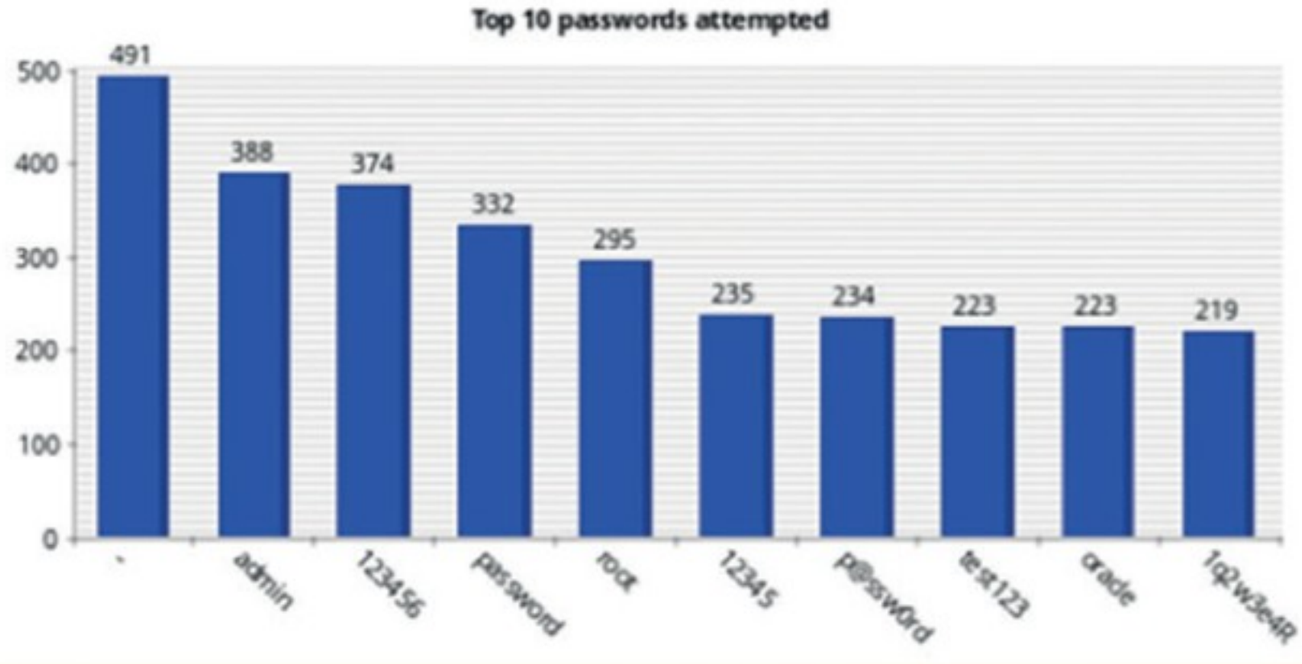


Figure 5. Kippo Top 10 Passwords Attempted

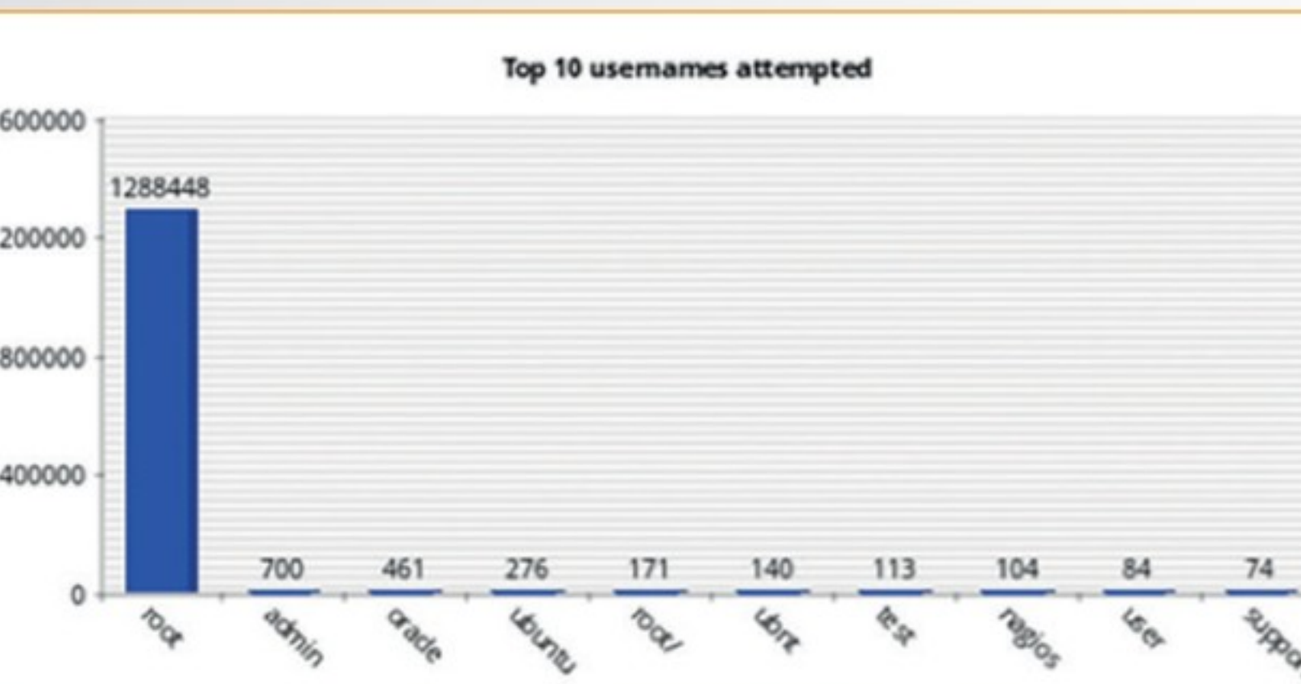


Figure 6. Kippo Top 10 Usernames Attempted

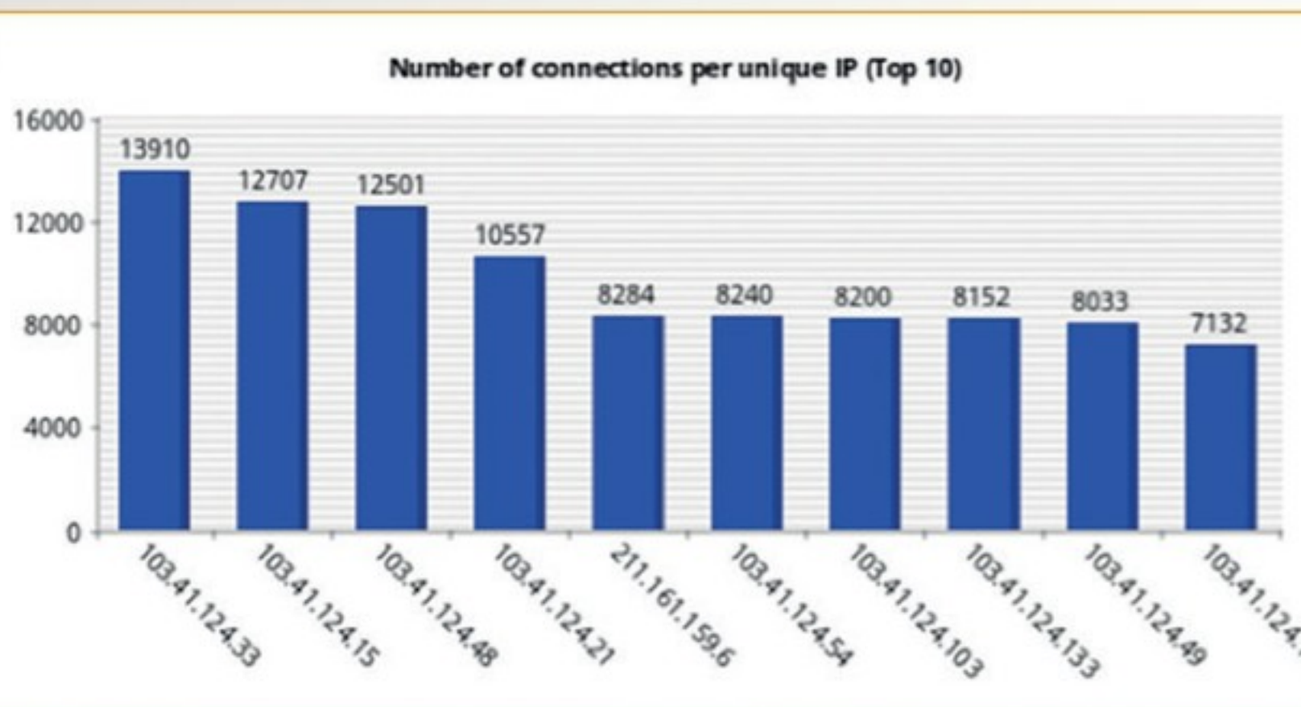


Figure 7. Kippo Top 10 Connections by Unique IP

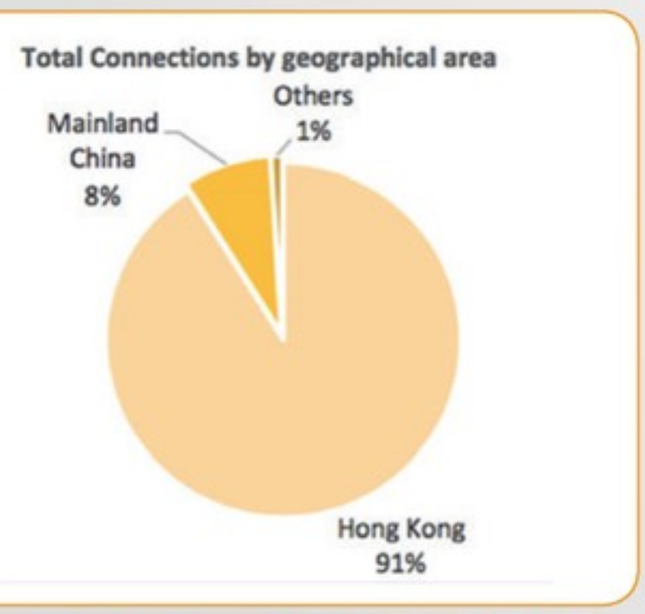


Figure 8. Kippo Top 10 IP by Geographical Area

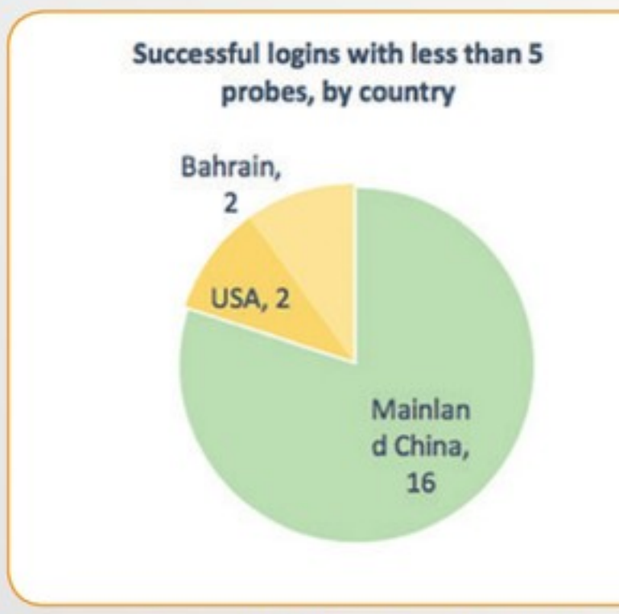


Figure 9. Successful Kippo Logins With Less Than 5 Probes by Country

/ METHODS OF ATTACK

The main passwords attempted were commonly known passwords. [Figures 5 & 6]

/ WHO IS ATTACKING?

The vast majority of probes (over 91%) came from the same region, which is identified as being a business address in the central Hong Kong area. [Figures 7 & 8]

There were a many successful logins with a small number of probes, for example there were 20 successful logins with less than 5 attempts. The majority of these IP are traced back to the Chinese mainland and were responsible for the majority of malware downloads. [Figures 9 & 10]

/ WHAT THE ATTACKERS DO ONCE INSIDE THE HONEYPOT

Most of the successful input are commands such as “uname” to find out details of the operating system and “chmod” commands to try to change permission. [Figures 11 to 14]

/ CHINESE ATTACK SERVER PANEL

One notable find was that one of the attackers left their server information when trying to download malware, which revealed a botnet creation and control panel. This panel was responsible for the download of one of the gates.6 malware samples. [Figure 15]

/ RESULTS PHASE 2 – DIONAEA

All four Dionaea honeypots ran uninterrupted except for occasional brief periods of maintenance. They ran between 20 March – 04 April 2015. [Figure 15]

/ COMPARISON BETWEEN INDIVIDUAL HONEYPOTS

All the honeypots except Ireland received over 2000 probes, yet Ireland still obtained 10 malware samples. [Figure 16]

/ COMBINED RESULTS

The honeypots received probes from 2385 IP addresses from a wide range of countries. The most popular being Argentina. [Figures 17 & 18]

“THE RESULTS SHOW THAT ALL THE FRONT END INPUTS OF THE WEB SERVER WILL BE CONTINUALLY PROBED EVERY DAY FOR VULNERABILITIES.”

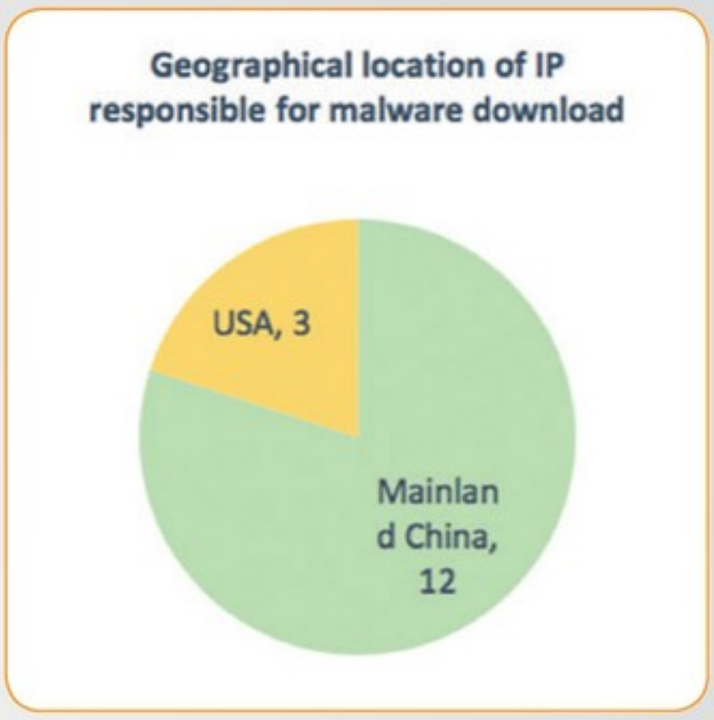


Figure 10. Location of Malware Dowload

The most common port attacked was 445 the smb port, followed by 1433 ms-sql, http and then 3306 mysql. [Figure 19]

/ MALWARE ANALYSIS

There were 51 malware samples obtained. The majority of the malware are generic worms and trojans and a lot of unknown or unrecognisable files. The recognised downloads are seen in Table 5.

/ GLASTOPF

Both Glastopf honeypots were deployed between 30/03/15 – 14/04/15, for a total of 16 days.

There were a total of 12,318 probes. Unfortunately the Ireland honeypot was largely ignored and most of its hits are from authentic web crawling bots like Googlebot. [Figures 20 & 21]

All the IP addresses starting with 66.249. are IP addresses of Google bots so they are not malicious probes. So six out of the top ten are Google bots, the other four are:

- 93.189.168.33 – Germany – 817 probes
- 87.69.252.21 – Israel – 761 probes
- 116.0.3.165 – Indonesia – 641 probes
- 5.34.183.81 – Ukraine – 592 probes

The following graphs show the requests made to try to gain access to the site including top in url requests, title requests and in text requests. [Figures 22 to 24]

/ DISCUSSION

The intensity and frequency of attack suggests that all 4 honeypots were subjected to brute force attacks at certain periods and the Sao Paulo honeypot was subjected to dictionary attacks almost continually.

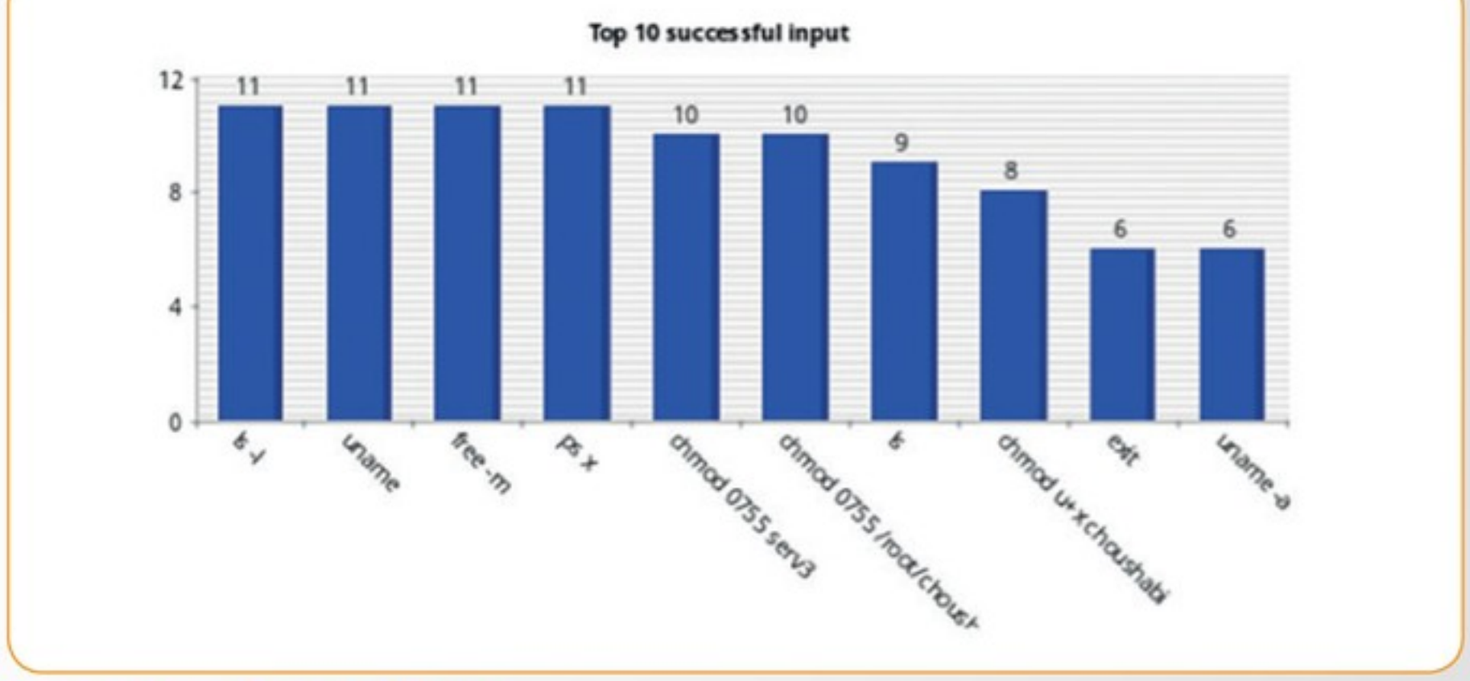


Figure 11. Top 10 Successful Input

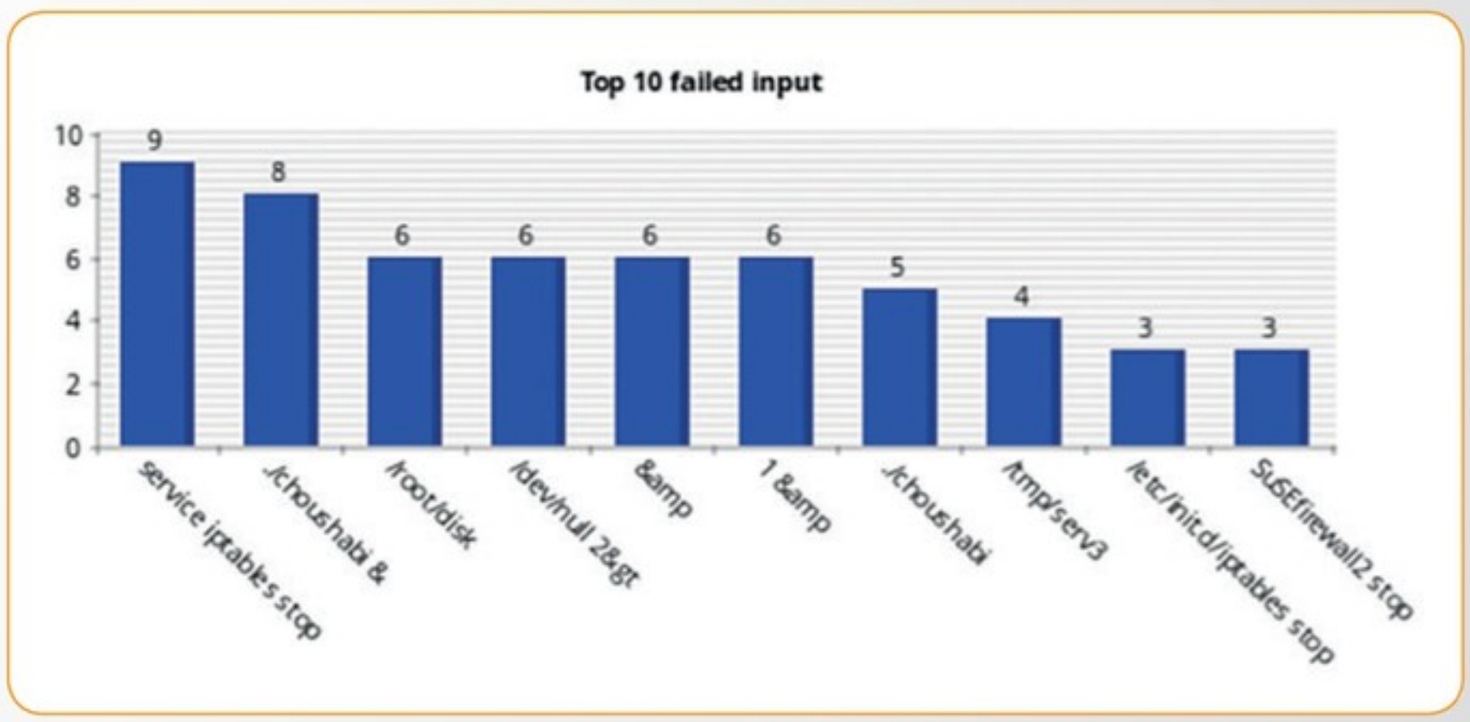


Figure 12. Top 10 Failed Input

Total login attempts:	**8517**
Distinct source IP addresses:	**2385**
URL downloads	**10**
Malware samples downloaded:	**51**

Table 4. Dionaea Results

Nickname	Hash	Type of file	Virus Total Results: names	Total downloads	Summary
Gates 6	a82081b270c7421d179f07bafa4d0873	ELF 32-bit executable	Linux.BackDoor.Gates.6 Unix.Trojan.Elknot Linux/DDoS-BD	5	Gates 6. Bill gates botnet DDoS linux trojan
Serv 3	c174fef4be0e66dc2816dfcb812b18fd	ELF 32-bit executable	Linux.DDOS.Flood.A ELF:MrBlack-A Linux/MrBlack	4	DDOS Flood MrBlack Linux specific Botnet
Gates 5	a61939ac4d71627e91475f7747dcef71	ELF 32-bit executable	Linux/DDoS-BD Linux.BackDoor.Gates.5 Unix.Trojan.Elknot	3	Gates 5. Bill gates botnet DDoS linux trojan
Chousabi	e0d35ea675c8ca58871a7211ab20de25	ELF 32-bit executable	Backdoor.Linux.Mayday.g Trojan[Backdoor]/Linux.Mayday Trojan.Unix.DDoS.dncljq	2	DDoS Target shellshock vulnerbailities
Cli 3	7082c8662a62d0fc178722ed5226f744	ELF 32-bit executable	Elf:Chinaz-C Linux/DDoS-BO Linux.DDoS.73	1	DDoS attack bot

Figure 13. Malware Downloads

Type of file	Hash	Name	Total downloads
PE32 – MS Windows	86b4e50393e52f0f649de6756b6f5f36	Trojan.agent Worm.generic.230976 Trojan.spy-win32.Agent.bbel	11
PE32 – MS Windows	1fab3fab216d9d5266249cb6ea2f918f	Worm.generic Trojan.win32.agent.bmgds W32/agent.IX.gen!Eldorado	7
Embedded PE32 – MS Windows	0007ff27c2cd405648cbbbdae8885742	Trojan.swizzor.1802 Worm.generic 44385 Trojan.win32.deborn	6
Embedded PE32 – MS Windows	d41d8cd98f00b204e9800998ecf8427e	Win32.Sality.E Win32/Sality.K Win32:Sality-U	5

Table 5. Dionaea Malware Samples

Words Bill and Gates found in the malware code

```
7CConfig
13CInitResponse
11CBillStatus
15CCommonResponse
11CUpdateBill
12CUpdateGates
8CLoopCmd
9CShellCmd
15CFakeDetectInfo
18CFakeDetectPayload
```

Attack vectors

```
11CAttackBase
13CPacketAttack
10CAttackUdp
10CAttackSyn
11CAttackIcmp
10CAttackDns
10CAttackAmp
10CAttackPrx
15CAttackCompress
10CTcpAttack
9CAttackCc
9CAttackIe
7CSerial
GLIBCXX_FORCE_NEW
127.0.0.1
vector::_M_insert_aux
vector::_M_fill_insert
```

Sample of IP address range

```
218.85.152.99      202.102.224.68
218.85.157.99      202.102.227.68
222.47.29.93       222.85.85.85
202.101.107.85     222.88.88.88
119.233.255.228    210.42.241.1
222.47.62.142      202.196.64.1
122.72.33.240      112.100.100.100
211.98.121.27      202.97.224.68
218.203.160.194    219.235.127.1
221.7.34.10        61.236.93.33
61.235.70.98       211.93.24.129
113.111.211.22     211.137.241.34
202.96.128.68      219.147.198.230
```

Figure 14. Strings Found in Code of Gates.5 Malware

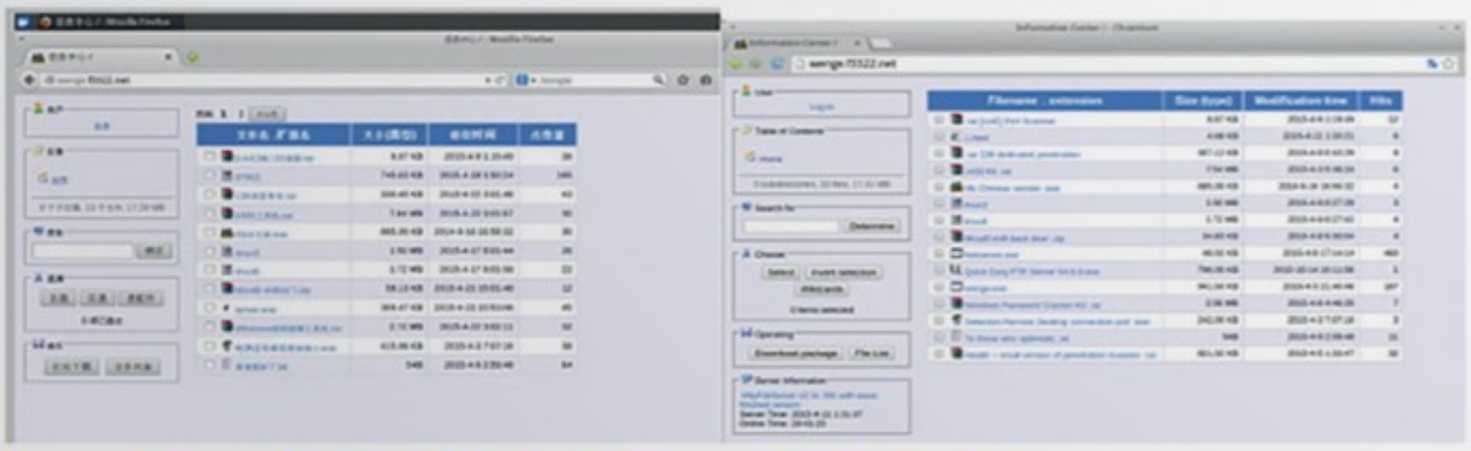


Figure 15. Botnet Attack Panel (Original Chinese and English Translation

All of the data such as IP addresses, usernames and passwords attempted can be useful for contributing towards intelligence to help maintain the security of systems and helps paint the picture of how such attacks are taking place. Also the commands used inside the honeypot help show what techniques hackers use to install malware.

/ COMPLETE ATTACK AND INFECTION PROCESS IDENTIFIED

The amount and frequency of attacks suggest that the majority of initial probes are by automated bots. But the video files which accompany all the successful malware downloads suggest that the majority of malware is downloaded by humans and the fact that there are many logins with few probes suggests that people are logging in with the information gained by the successful brute force attacks.

Therefore results show that there are usually three separate IP addresses used in the infection process.

1. The IP responsible for the brute force attack to guess the password, most probably used by a bot or script
2. The IP used by the human logging in using the information gained by the brute force attack
3. The IP address where the human downloads malware from (at least in one instance this was from an attack panel as shown in Figure 25)

/ FINDINGS FROM MALWARE ANALYSIS

During 2014 a number of anti-virus companies started to highlight the increasing threat of Linux targeted malware and botnets, especially Linux DDoS Trojans. (Dr.Web, 2014) (Kaspersky Publications, 2014) It was also suggested that the malware is primarily being distributed from Chinese based web panels (similar to the one in Figure 25). (Malware Must Die, 2014)

All of the malware samples identified in this study are Linux specific malware DDoS flood type botnet Trojans. Over half have been recognised as Gates .5 or .6. which has been identified as belonging

to the Bill Gates botnet which is a Linux specific botnet, identified by the words 'Bill' 'Gates' in the string in the code of the malware. Which overall seems to confirm the suggestions made by the anti-virus companies mentioned that there is an increasing threat of Linux targeted malware and botnets.

/ PHASE 2 – DIONAEA FINDINGS

While there was a variance between the amount of attacks on all four honeypots, each one obtained payload and malware samples.

The attacks on the Windows emulation came from many different areas of the world, with the most attacks coming from Argentina. This suggests that the servers being used in such attacks are pretty much world-wide and it is not possible to specify one geographical area of danger.

The attacks by port statistics give some useful information about where the threats are targeted, with by far the most targeted port being port 45 smb with 57% of attacks, but other ports such as 80 http, 1433 ms-sql, and 3306 mysql received attention.

/ MALWARE ANALYSIS

Overall the honeypots collected 51 malware samples in 16 days which gives an indication of the sorts of threats that such systems face. The majority of the malware was generic Trojans and spyware.

/ GLASTOPF FINDINGS

Unfortunately because the Ireland honeypot didn't get much attention the majority of the findings come from just one honeypot, which isn't the most statistically reliable way to draw conclusions. Also the honeypots received a lot of probes from web service bots that need to be filtered out. Yet the data still gives some indication of the sorts of threat and attacks that web-servers regularly face.

The results show that all the front end inputs of the web server will be continually probed every day for vulnerabilities, the most common types of probe are requests in the URL space with hundreds of attempts to break into the server, while the other form input spaces receive a wide range of queries.

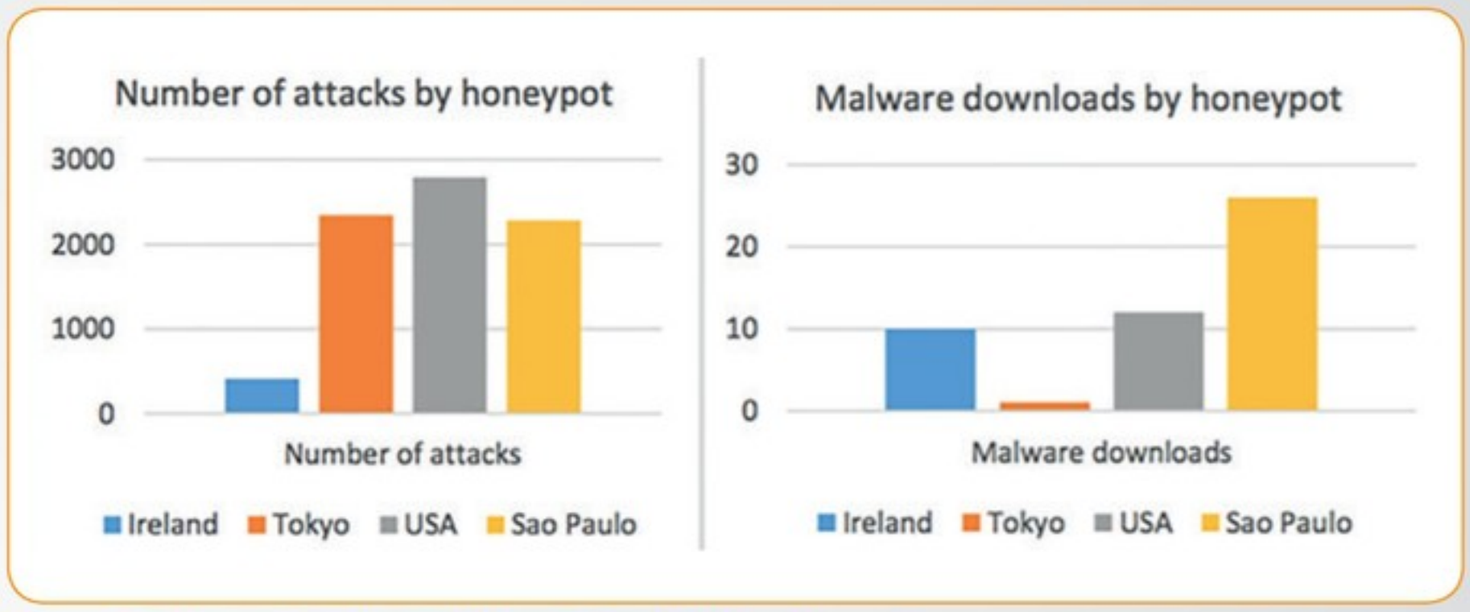


Figure 16. Dionaea Attacks & Malware Downloads by Honeypot

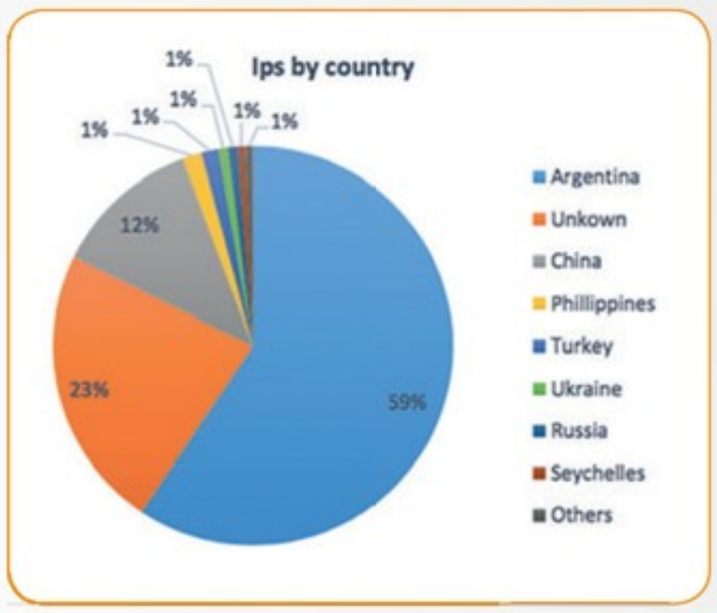


Figure 17. Dionaea IP by Country

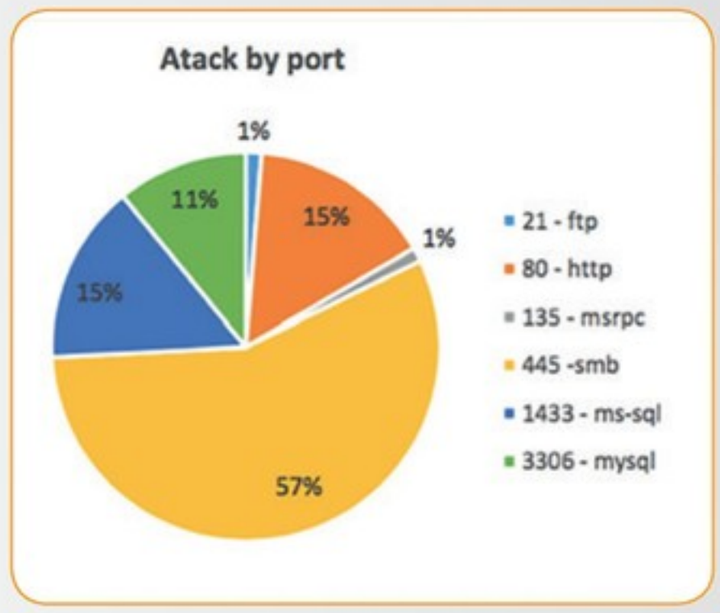


Figure 18. Dionaea Top 10 Attackers

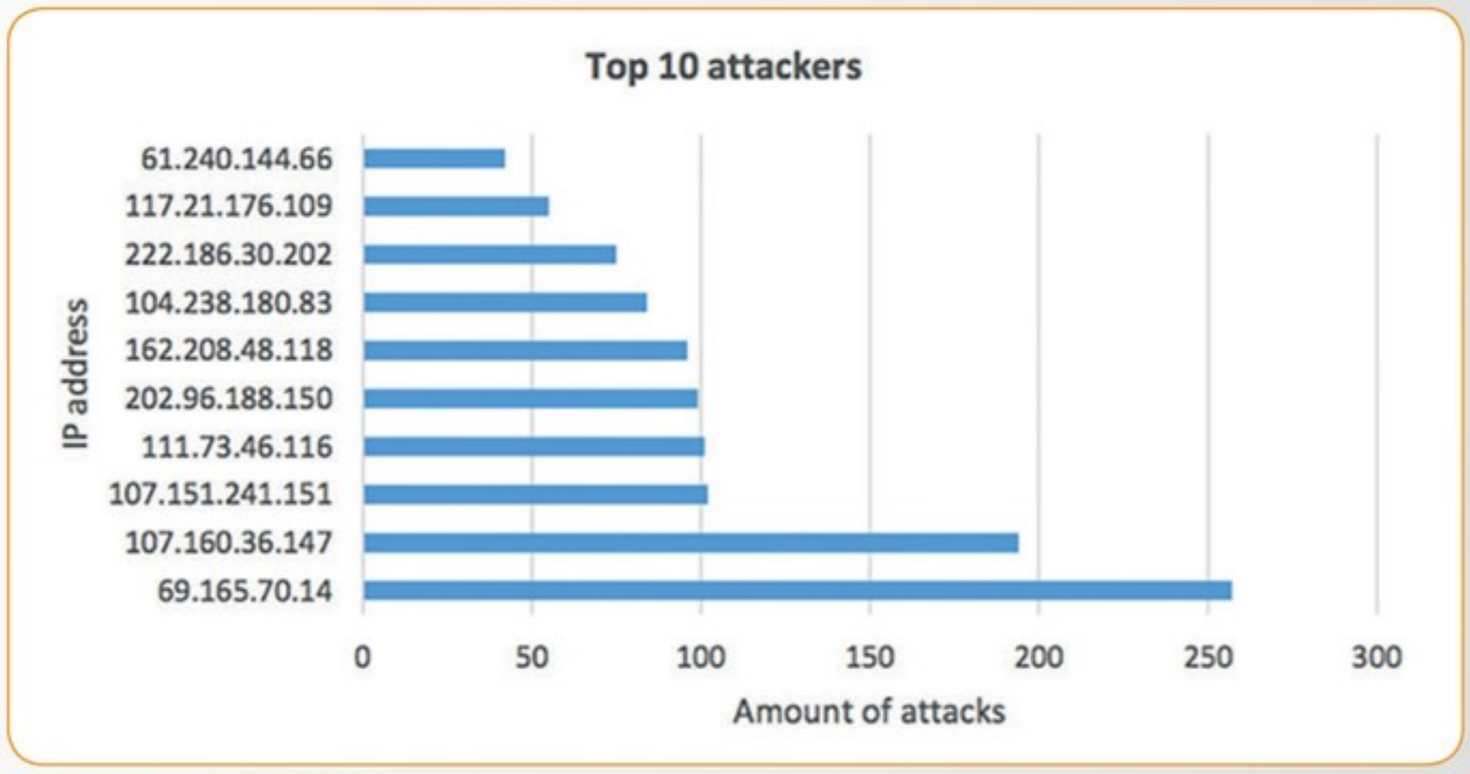


Figure 19. Attack By Port

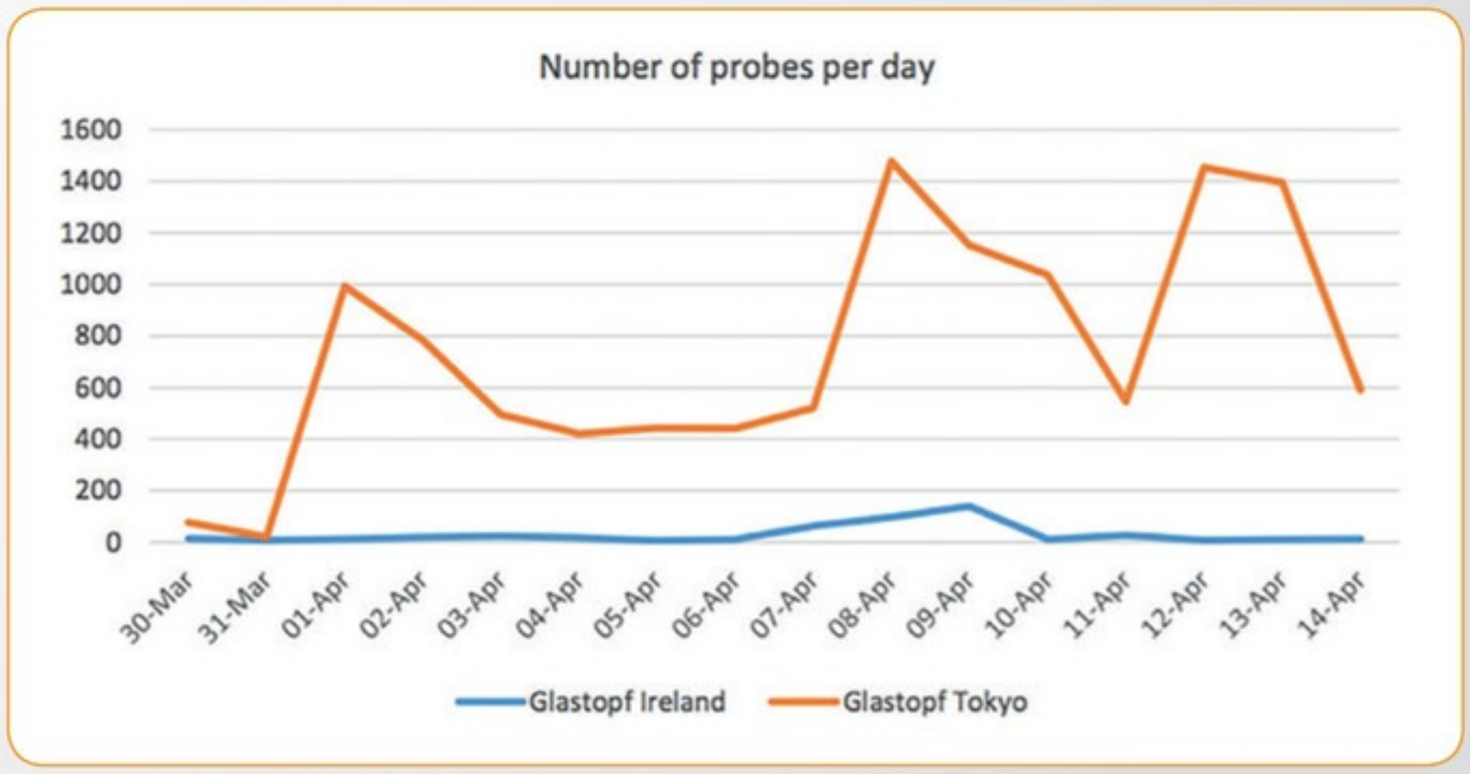


Figure 20. Glastopf Probes Per Day

/ FINDINGS THROUGH HONEYPOT COMPARISON

Due to the wide variety of results between the different instances of the same honeypot deployment it is clearly shown that data is going to be more reliable and useful if honeypots are deployed at a wider scale.

For example with the Kippo honeypots the SaoPaulo instance had an enormous amount of attacks but very little data from inside the honeypot, while Japan had far less attacks but more successes and malware samples.

With Dionaea the Ireland honeypot had very few attacks and probes but still collected a comparably high amount of malware samples, whereas the Tokyo instance obtained very few samples. And the Glastopf Ireland instance didn't manage to obtain any useful data at all.

/ CONCLUSIONS

The study was limited to three types of honeypot and one cloud provider, so it is difficult to extrapolate the results as being relevant to all systems on the internet and all cloud providers, yet all three types of honeypot gathered useful data which can be used for intelligence in the fight against malware distribution.

In particular the Kippo deployment gathered a lot of useful information about the infection process of systems through port 22 SSH, including up to date new threats, as well as much generalised information about how attacks take place.

The Dionaea honeypot also recorded a lot of valuable information and obtained a lot of malware samples, which can be reverse engineered for valuable intelligence. While the Glastopf deployment results are not as statistically reliable, the results still give an indication of the sorts of threats typical web servers face and certainly further research could be done in the future with the Glastopf honeypot.

The installation of Kippo and Dionaea honeypots was not completely straightforward. Both required a lot of experimentation to configure correctly, while Kippo became a lot easier. After a time the first round of Dionaea honeypots had to be scrapped and rebuilt. Glastopf proved to be considerably easier.

When extracting information all the honeypots had a mysql type database

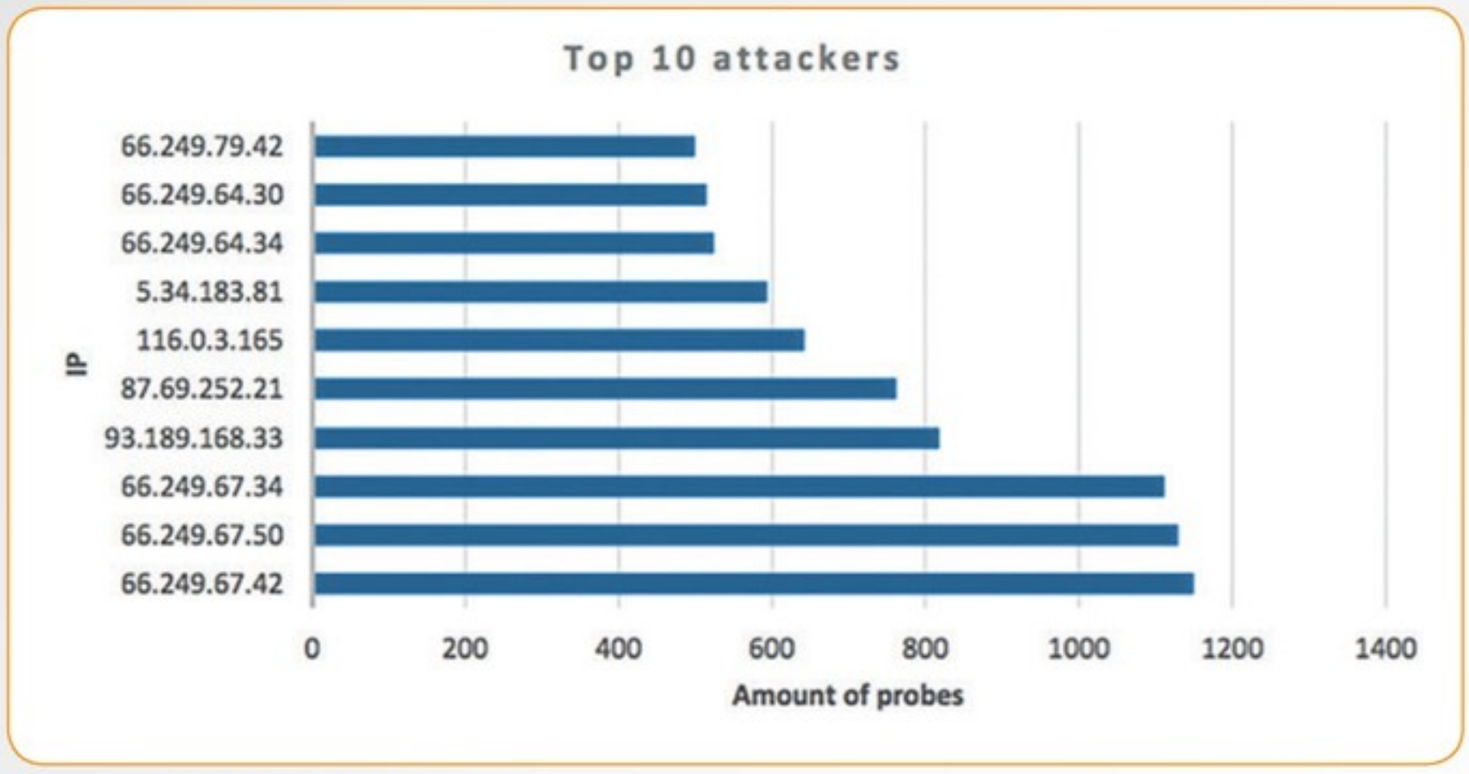


Figure 21. Glastopf Top 10 Attackers

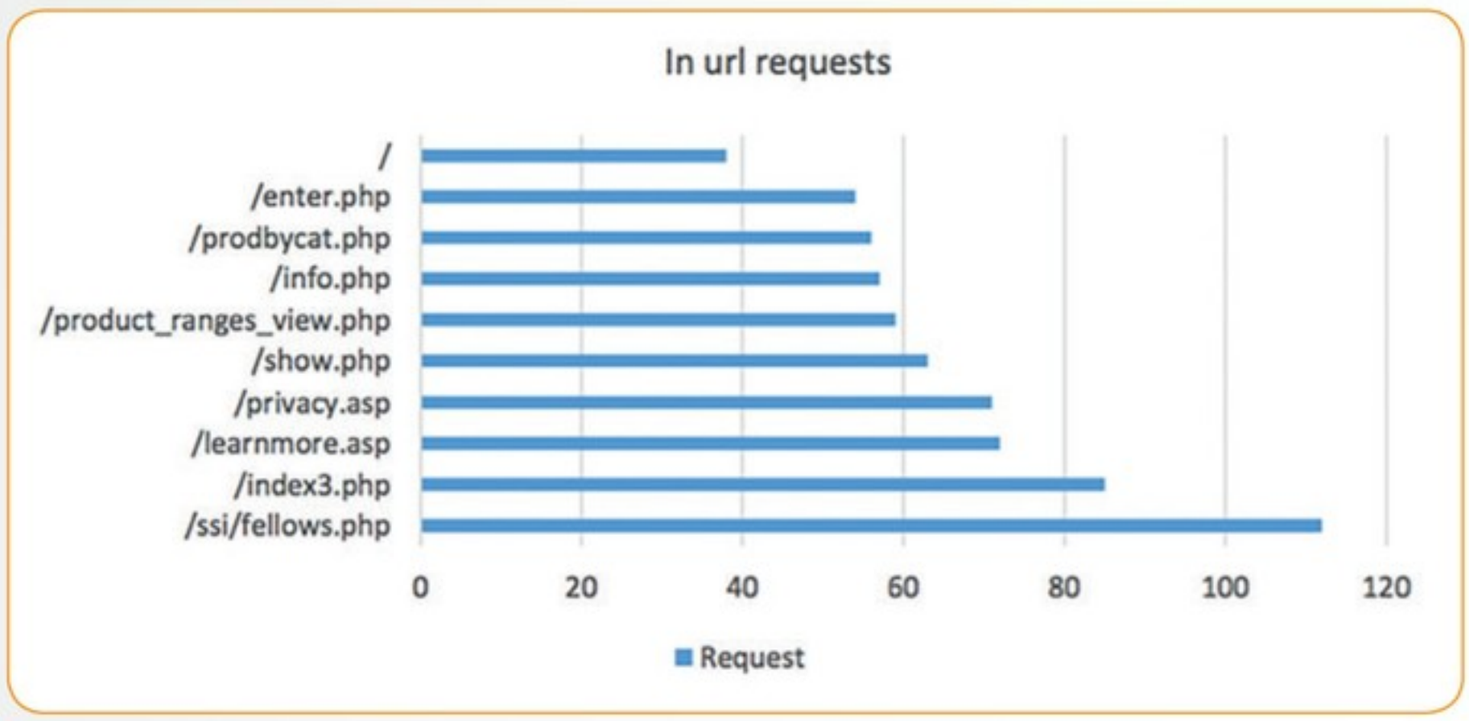


Figure 22. Glastopf Top In Url Requests

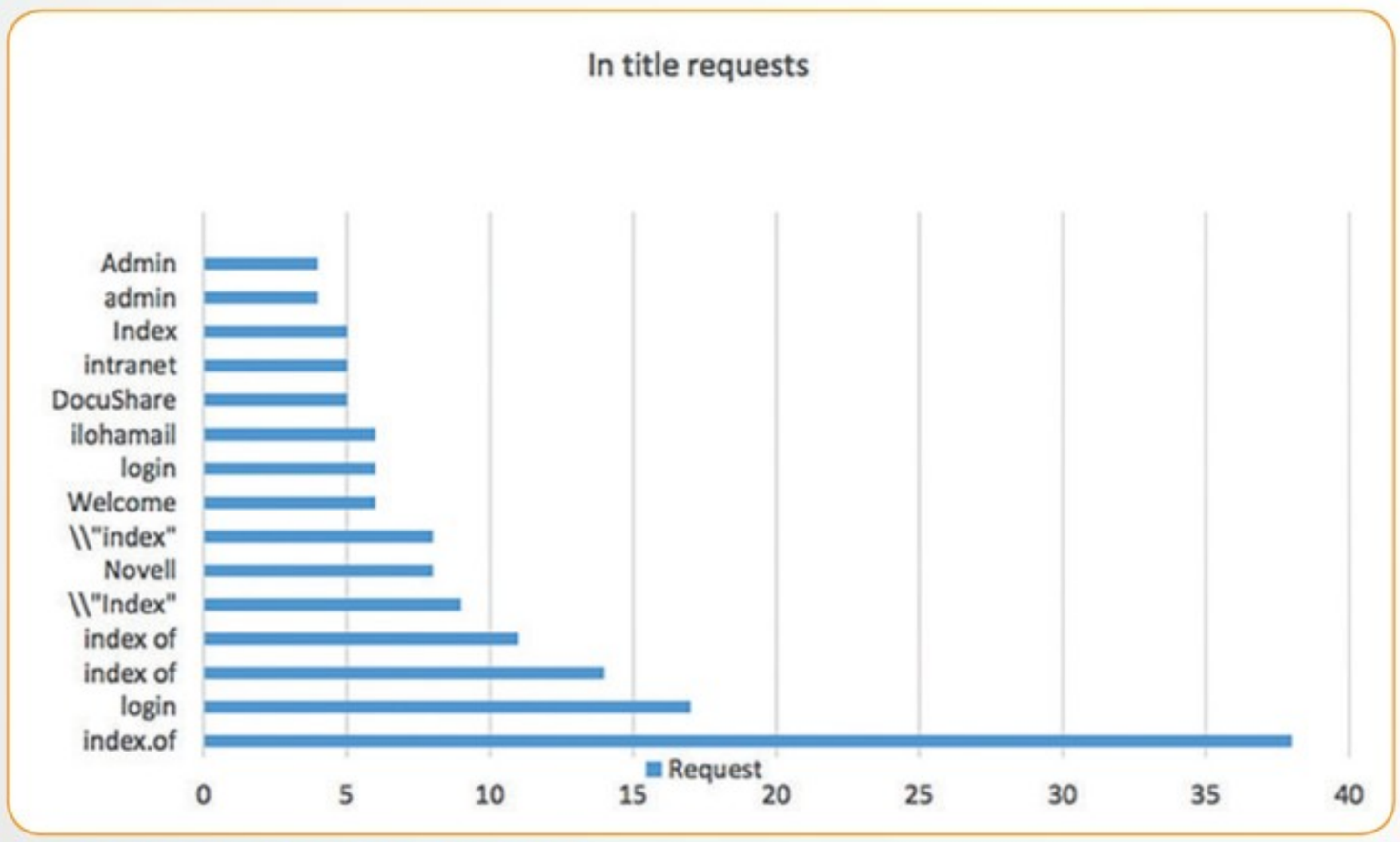


Figure 23. Glastopf Top in Title Requests

"THE DIONAEA HONEYPOT ALSO RECORDED A LOT OF VALUABLE INFORMATION AND OBTAINED A LOT OF MALWARE SAMPLES, WHICH CAN BE REVERSE ENGINEERED FOR VALUABLE INTELLIGENCE."

which meant their databases were easily accessible. For Kippo the use of Kippo-Graph was particularly useful as an efficient management tool. Similarly the Dionaea FR management tool provided some automation of statistics although not with as much detail as is ideal and it proved more difficult to configure. Glastopf had no management tool.

Therefore it was found that on an individual honeypot basis extracting meaningful data was reasonably straightforward, but when it came to pooling the data from all the honeypots to obtain overall statistics the process proved difficult and the process was laborious. So the more honeypots deployed the more it clearly becomes a "big data" problem to extract the relevant information. So in that sense there is a scalability issue when deploying a large number of honeypots.

Solutions to this issue in the future could be through the use of customised big data tools to pool the data. Or an alternative approach could be to configure the honeypots to send a summary detail report to the central server, for example the OWASP Distributed Honeypot project uses an XML report for this process.

REFERENCES

Challoo, R., Kotapalli, R. 2011. Detection of botnets using honeypots and p2p botnets. Journal of Computer Science and Security. [e-journal]. Available through: Google Scholar website: https://scholar.google.co.uk/ [Accessed 02 April 2015]

Choubey, R., Dubey, R., Bhattacharjee, J. 2011. A Survey on Cloud Computing Security Challenges and Threats. International journal on computer science and engineering (IJCSE). [e-journal] . Available through: Anglia Ruskin University Library website: http://libweb.anglia.ac.uk [Accessed 12 April 2015]

Jang-Jaccard, J., Nepal, S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. [e-journal] 80. PP 973-993. . Available through: Anglia Ruskin University Library website: http://libweb.anglia.ac.uk [Accessed 9 April 2015]

Kumar, S., Sehgal, R., Singh, P., Chauhyary,A., 2012. Nepenthes Honeypots based Botnet Detection. Journal of Advances in Information Technology. [e-journal] 3(4). pp. 215-221. Available through: Anglia Ruskin University Library website: http://libweb.anglia.ac.uk [Accessed 01 February 2015]

Mansfield-Devine. 2011. DDoS: threats and mitigation. ScienceDirect (Elsevier B.V.). [e-journal] 12 pp5-12. . Available through: Anglia Ruskin University Library website: http://libweb.anglia.ac.uk [Accessed 16 April 2015]

Shimoda, A., Mori, T,. Goto, S,.2010. Sensor in the Dark: Building Untraceable Large-scale Honeypots using Virtuallization Technologies. 10th Annual International Symposium on Applications and the Internet. [e-journal] Available through: Anglia Ruskin University Library website: http://libweb.anglia.ac.uk [Accessed 04 March 2015]

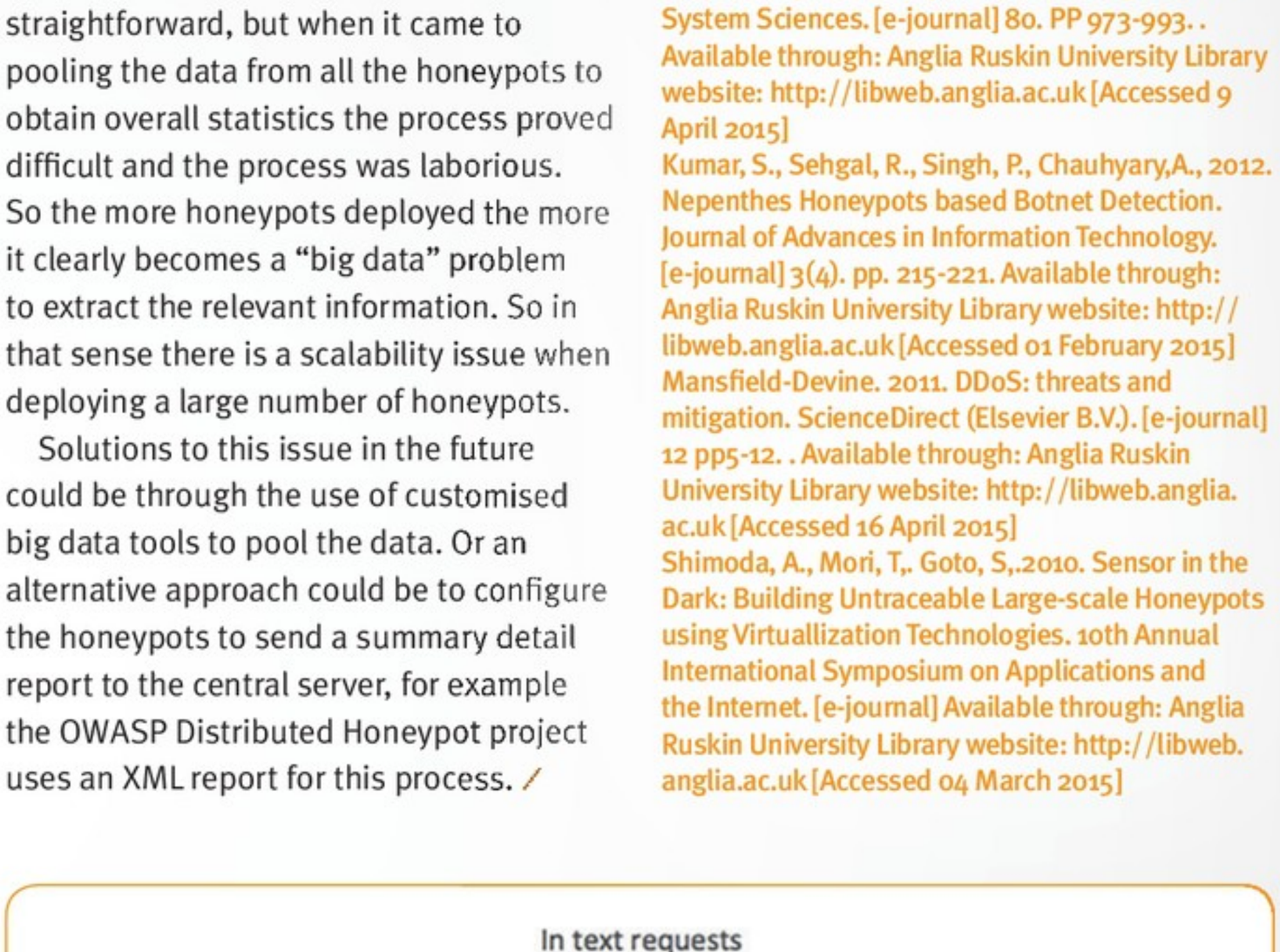


Figure 24. Glastopf Top in Text Requests

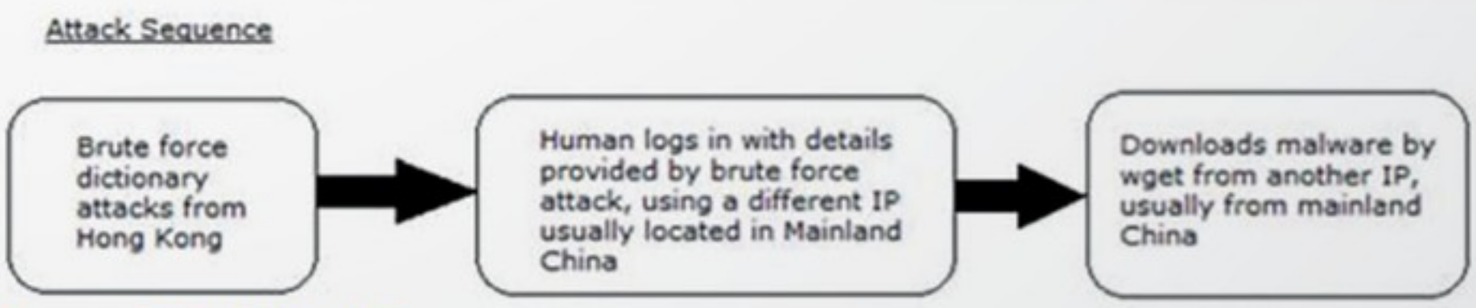
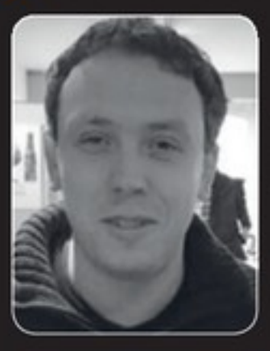


Figure 25. Typical Attack Sequence

AUTHOR BIOGRAPHY

Adrian Winckles is Course Leader/ Senior Lecturer for BSc(Hons) Information Security and Forensic Computing and Security Researcher at Anglia Ruskin University. He is OWASP Cambridge Chapter Leader, OWASP Europe Board Member and is involved in rebooting the Cambridge Cluster of the UK Cyber Security Forum. His security research programs include (in)security of software defined networks/everything (SDN/ Sdx), novel network botnet detection techniques within cloud and virtual environments, distributed honeypots for threat intelligence, advanced educational techniques for teaching cybercrime investigation and virtual digital crimescene/incident simulation. He has successfully completed a contribution to the European FP7 English Centre of Excellence for Cybercrime training, research and education (ECENTRE). He is vice chair of the BCS Cyber Forensics Special Interest Group.

AUTHOR BIOGRAPHY



Simon Clary is a recently graduated Masters student in Information and Communication Technology from Anglia Ruskin University. BA from Manchester University. Member of the Cambridge chapter of The Open Web Application Security Project (OWASP).